Anatomy of a Computer Intrusion

If you suspect your facility's technology or information has been targeted, report it to your FSO or security point of contact.

The following steps outline the methods attackers commonly use to launch cyber attacks.

1 Reconnaissance

Attackers research and identify individuals whom they will target through open source means.

2 Intrusion into the network

Attackers send spear-phishing emails to targeted users within the company with spoofed emails that include malicious links or attached malicious documents.

3 Obtain user credentials

Attackers get most of their access using valid user credentials. The most common type: domain-administrator credentials.

4 Establish a backdoor

With domain administrative credentials, the attackers will move laterally within the victim's network, installing backdoors for future and continued exploitation.

5 Install multiple utilities

Utility programs are installed on the victim's network to conduct system administration, steal passwords, get email, and list running processes.

6 Data exfiltration

The attackers obtain emails, attachments, and files from the victim's servers and then encrypt and exfiltrate the data via the actor's Command & Control infrastructure.

7 Maintaining persistence

If the attackers suspect they are being detected or remediated, they will use other methods to ensure they don't lose their presence in the victim's network, including updating their malware.